



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE**

SEMIANNUAL REPORT TO THE CONGRESS

October 1, 1999 through March 31, 2000

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 31032000	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i> 01101999 31032000
Title and Subtitle Semiannual Report to the Congress		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General DOD		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms "IATAC COLLECTION"		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 54		

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 3/31/00	3. REPORT TYPE AND DATES COVERED Report		
4. TITLE AND SUBTITLE Inspector General's Semiannual Report to the Congress		5. FUNDING NUMBERS		
6. AUTHOR(S) DoD				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060		10. SPONSORING / MONITORING AGENCY REPORT NUMBER		
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words)				
14. SUBJECT TERMS Information, Security			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	

FOREWORD

It is my pleasure to report on the accomplishments of the Office of the Inspector General, Department of Defense, for the period October 1, 1999, through March 31, 2000. This Semiannual Report summarizes significant Department-wide audit and investigative efforts. Oversight projects relating to the intelligence community are discussed in a separate classified annex.

The Highlights section provides an overview of the most significant issues discussed in the report. Chapter One contains brief updates on what we consider to be the Department's principal high-risk areas. We have also included a more detailed discussion of a special emphasis area—Information Assurance. Chapter Two includes discussions of other important audit and investigative efforts that took place during the period, again resulting in significant criminal prosecutions and the identification of large dollar savings and recoveries.

Year 2000 conversion dominated our efforts during this reporting period culminating in an uneventful transition to the new year. Although some system problems were noted, our comprehensive effort complemented Department actions to ensure that no mission critical failures occurred. Responding to issues of critical interest to Congress and the Department contributed toward making this an especially busy reporting period. We testified before the Senate regarding the personnel security investigations backlog and export control issues and before the House regarding the top 10 principal management challenges facing the Department, as well as significant Defense acquisition management issues. We also provided reports to requesting congressional committees and members covering a wide array of issues including the anthrax vaccine, chemical protective suits, the Civil Air Patrol, information technology, and general and flag officer housing. Additionally we commented on proposed legislation for the Department's Authorization Act, the Government Information Security Act, and the Export Administration Act.

In our last report I indicated that, although the Department budgeted for urgently needed additional resources, the Congress reduced our fiscal year 2000 appropriation. To meet increasing demands placed on our agency by both Congress and the Department, I again ask that our resource requirements forwarded in the fiscal year 2001 President's Budget be supported. This support is essential to restoring much needed coverage to high-risk areas with an appropriate level of responsiveness. Additionally, we have operated without an Inspector General for an entire year.

As an example of the many unprogrammed projects we are called on to perform, on December 13, 1999, the Secretary of Defense tasked the Office of the Inspector General to assess the environment with respect to the application of the Department's homosexual conduct policy, commonly referred to as "Don't Ask, Don't Tell." Within 90 days, our auditors and evaluators developed an appropriate survey, visited 38 military installations and 11 Navy ships, administered over 71,500 surveys and produced the *Report on the Military Environment with Respect to the Homosexual Conduct Policy*. This report has elicited a positive response, and is being used by the Department to more effectively address this sensitive area.

The men and women of the Office of the Inspector General are committed to providing a level of oversight to the Department of Defense that materially contributes to the safety, efficiency and effectiveness of our Nation's Armed Forces.

Donald Mancuso
Deputy Inspector General

This page left blank intentionally

TABLE OF CONTENTS

HIGHLIGHTS	i
Introduction	i
Information Assurance	ii
Other Activities	ii
 CHAPTER ONE – REDUCE HIGH RISK VULNERABILITIES	 1
Introduction	1
Acquisition	1
Financial Management	3
Infrastructure	4
Information Technology	5
 Special Emphasis Area--Information Assurance	 7
Recent Audit and Inspection Results	8
Future Activity	10
Policy Still Evolving	11
Summary	12
 CHAPTER TWO - SIGNIFICANT ACTIVITIES	 13
Introduction	13
Criminal Investigations	13
Hotline	21
Administrative Investigations	21
Criminal Investigative Policy and Oversight	26
Auditing	27
Intelligence Review	31
 APPENDICES	
A. Reports Issued by Central DoD Internal Audit Organizations	A-1
B. Inspector General, DoD, Audit Reports Issued Containing Quantifiable Potential Monetary Benefits	B-1
C. Followup Activities	C-1
D. Contract Audit Reports Issued	D-1
 FIGURES	
1. Defense Criminal Investigative Organizations Case Results	14
2. Military Whistleblower Reprisal Cases Open as of March 31, 2000	23

3.	Whistleblower Reprisal Cases by Category of Employee Open as of March 31, 2000	23
4.	Program Integrity - Senior Official Inquiries Open as of September 30, 1999	25
5.	Program Integrity - Nature of Substantiated Allegations Against Senior Officials During 1st Half FY 00	25
6.	Intelligence Oversight	31

HIGHLIGHTS

INTRODUCTION

During the 6-month period ending March 31, 2000, the Office of the Inspector General, Department of Defense, (OIG, DoD), continued to place emphasis on reducing vulnerabilities and improving controls in the principal high risk areas in the Department: Acquisition, Financial Management, Infrastructure and Information Technology. In addition, the OIG, DoD, gave special emphasis to the area of Information Assurance.

Acquisition

In fiscal year 1999, the DoD purchased about \$140 billion of goods and services with 14.8 million purchase actions, about 57,000 on an average working day. The DoD internal audit agencies issued 25 reports on acquisition management. The audit results underscore the need to continue efforts to strengthen acquisition reform efforts, improve DoD acquisition policies and practices, place more management emphasis on processes for managing contracts for services and dealing with workforce management issues and the impact of reductions on the DoD acquisition workforce.

Financial Management

Although the DoD continues to make progress toward compliance with the new Federal accounting standards, the audit results for the fiscal year 1999 financial statements were no better than for previous years. The core problem continues to be that the DoD lacks the financial and feeder systems needed to compile financial statements in accordance with applicable standards. The DoD audit agencies devoted more than 400 work-years to financial statement audits. Of the 57 reports issued on financial management, over 40 focused on financial statements.

Infrastructure

Many ongoing logistics reform initiatives focus on problems identified in previous audit and inspection reports but it is imperative that robust oversight efforts continue in this area. Infrastructure includes at least three areas where the risk of waste and fraud is especially high: property disposal, health care and environmental cleanup. During the reporting period, DoD auditors issued 41 reports on construction, other facilities issues, environmental programs, health care, supply and maintenance. Investigative efforts in these areas are also highlighted.

Information Technology

The Y2K computing problem posed a huge challenge in terms of its scope, because all 10,000 DoD networks and 2.5 million computers were potentially affected. The DoD Y2K conversion effort was extremely successful. Only a few system failures occurred, operational impact was insignificant and surprisingly few problems occurred in supply chains and infrastructure. The numerous findings in over 200 reports issued on Y2K

conversion, as well as the hundreds of corrective actions taken in response to those reports, identified many risks that the Department ultimately was able to minimize. During this semiannual period, DoD auditors issued 35 reports on information technology issues; 28 addressed Y2K issues. With the completion of the Y2K conversion, the oversight community needs to provide more coverage of other information technology issues. The most formidable of the known challenges in the area of information technology relate to ensuring the security of networked systems and overcoming a legacy of overly decentralized and poorly controlled information systems management.

INFORMATION ASSURANCE

The Y2K effort by the DoD audit organizations and the Service Inspector General offices left relatively few resources for information assurance coverage. Nevertheless, more than 20 reports were issued on the subject between January 1999 and March 2000. Those reports pointed out the need for a well-structured program with clear policies and metrics, as well as more aggressive measures to deal with chronic laxity in basic security procedures.

OTHER ACTIVITIES

During this reporting period, the investigative community was highly successful with 249 indictments and over \$500 million in monetary outcomes in fraud investigations. Also, the DoD Hotline received 6,245 telephone calls, letters and electronic mail reporting fraud, waste and mismanagement in DoD operations. The Hotline initiated 1,263 cases from the information provided. Since 1982, over \$419 million have been recovered as a direct result of information provided to the Hotline.

CHAPTER ONE – REDUCE HIGH RISK VULNERABILITIES

INTRODUCTION

The size, complexity and mission of the Department of Defense (DoD) create a wide range of management challenges, many of which are exacerbated by the numerous outmoded or inefficient systems and processes that have not yet been improved or replaced. Management reform and process reengineering were emphasized in all DoD functional areas throughout the 1990's, but it is evident that several more years of concerted effort will be required to achieve a wide range of statutory reform requirements and DoD management improvement goals. Due to their inherent characteristics and incomplete reforms, most DoD "business" operations, such as vendor pay and property disposal, must be considered high-risk activities. In this report, we provide updates on challenges and oversight activity in the broad high-risk areas of Acquisition, Financial Management, Information Technology Management and Infrastructure. We also discuss one new Special Emphasis Area—Information Assurance.

ACQUISITION

During fiscal year 1999, the DoD purchased nearly \$140 billion of goods and services with 14.8 million purchase actions, about 57,000 on an average working day. This huge scale makes oversight of DoD acquisition programs extraordinarily difficult. The DoD internal auditors issued 25 reports on acquisition during this 6-month reporting period. The audit results underscore the need to continue DoD efforts to strengthen the four pillars of a successful acquisition effort, which are:

- Sound processes for determining requirements.
- A consistent and reasonable framework of laws and regulations.
- Efficient processes incorporating sufficient management controls to ensure that desired results are achieved.
- A sufficiently sized, highly trained and motivated acquisition workforce.

More can be done to improve DoD acquisition policies and practices in all four areas. Regarding requirements determination, for example, in a February 2000 report, we noted that few significant improvements had been made to the guidance and models used to calculate needed quantities of munitions, despite 20 audit reports over 5 years, indicating problems. Systemic weaknesses include inconsistencies between Services,

questionable planning factors and lack of verification, validation and accreditation of models. Part of the problem appears to be ambiguity about what office is responsible for updating guidance and assessing the realism of planning scenarios and weapon utilization factors used in models.

The Department is still attempting to implement existing acquisition reform legislation. In some areas, regulatory or policy guidance needed to achieve legislative and management goals is lacking. For example, the DoD made reduction of the amount of Government-owned equipment in the possession of contractors a major goal in 1997, but has been unable to finalize the regulatory changes needed to end the longstanding practice of taking title to equipment for which there is little likelihood of further need.

Numerous initiatives are under way to seek acquisition process improvements. Some involve adopting commercial practices and many are focused on using new information processing and communication technology to reduce paperwork and speed up various phases of the acquisition cycle. Recently the central organization for contract administration was split off from the Defense Logistics Agency (DLA) as the independent Defense Contract Management Agency. Conceptually, this realignment should help both agencies by allowing DLA to concentrate on logistics and removing an organizational layer in the contracting community.

“An extensive audit of 105 contracting actions...showed flaws in all of them.”

Recent audits have indicated a clear need for DoD to put more management emphasis on processes for managing contracts for services, which now cost over \$50 billion annually and constitute a huge procurement program in their own right. Historically, acquisition reform efforts and training for both contracting and program management personnel have been heavily skewed toward acquiring hardware. An extensive audit of 105 contracting actions for professional administrative and management support services showed flaws in all of them. For example, Government cost estimates were inadequate for 77 percent of the actions.

Workforce management issues are now receiving much more attention in DoD and elsewhere in Government. In DoD, recruiting, retention and training problems exist for both civilian and military personnel. A recent audit raised significant concerns about the impact of reductions on the DoD acquisition workforce, which has been cut by over half without the forecasted reduction in workload. The number of contracting actions over

\$100,000 actually increased by 28 percent from fiscal years 1990 to 1999.

“A decade of downsizing...has left the DoD acquisition workforce understaffed and without a good balance between experienced and new employees.”

This mismatch between resources and workload is already having an impact on productivity, and will likely get worse because of the projected retirement of over 40 percent of the workforce over the next 5 years. A reasonably sized, well trained and highly motivated workforce is probably the most important factor in avoiding waste and increasing efficiency in DoD acquisition programs. A decade of downsizing and poor planning has left the DoD acquisition workforce understaffed and without a good balance between experienced and new employees. Drastic workforce reduction, if unaccompanied by process changes that decrease workload proportionately, is counterproductive. The DoD must do a much better job of understanding what drives the workload, realistically assessing the likely impact of process changes and determining what staffing resources and skills are needed.

FINANCIAL MANAGEMENT

The Chief Financial Officers Act of 1990 and related legislation require extensive audits of DoD annual financial statements. The Office of Management and Budget (OMB) requires the Department to compile and audit not just financial statements for the DoD as a whole, but also statements for 10 major subentities, such as the Army General Fund and Air Force Working Capital Fund. The Chief Financial Officer, DoD, is also pressing Defense agencies to prepare audited financial statements. Unfortunately, the DoD lacks accounting systems that can generate financial statements and must rely on a patchwork of innovative, but fundamentally inefficient and workload intensive procedures for compiling required data. The Military Department and OIG, DoD, audits of DoD financial statements for fiscal year 1999 identified an unbelievable \$7.6

“Unfortunately, the DoD lacks accounting systems that can generate financial statements and must rely on a patchwork of...procedures for compiling required data.”

trillion in accounting adjustments. Of the \$5.8 trillion of adjusted entries that were audited, \$2.3 trillion were unsupported by reliable documentation and audit trails. Accounting entries to complete or correct financial statements are rare in the private sector and unsupported entries are strictly forbidden.

Although the DoD continued to make progress toward compliance with the new Federal accounting standards, the audit results for the fiscal year 1999 financial statements were no better than for previous years.

Again this year, the Military Retirement Fund statements received an unqualified audit opinion, but disclaimers were necessary for all other DoD funds. The core problem continues to be that the DoD lacks the financial and feeder systems needed to compile financial statements in

accordance with applicable standards. The controls in existing systems are simply inadequate. Even huge and costly efforts to “audit in” the correct data and documentation, such as were attempted by the Army and Air Force over the past year, cannot compensate for the underlying system problems.

“Even with limited coverage...the DoD needs to keep working to improve management controls just to meet fundamental requirements....”

The DoD internal audit community devoted over 400 workyears to financial statement audits during the past cycle. Of the 57 reports issued on financial management, over 40 focused on financial statements. Other high-risk areas of concern, such as payments to contractors, received very limited audit coverage. Even with limited coverage, it remained evident that the DoD needs to keep working to improve management controls just to meet fundamental requirements, such as posting obligations when they are incurred, avoiding disbursement errors and reducing vulnerability to fraud.

The OIG, DoD, welcomed the recent Defense Finance and Accounting Service (DFAS) decision to upgrade its Internal Review Office. Management must do more to monitor the correction of previously identified weaknesses in the hundreds of processes involved in Defense finance and accounting activities. A stronger Internal Review Program should be helpful in this regard.

INFRASTRUCTURE

The Department has initiated several hundred actions to make its logistics programs more efficient and less costly. In March 2000, the Department issued guidance intended to place even more effort on this area, especially by the Military Departments. The six reemphasized reform goals are:

- Optimize support to the warfighter.
- Improve strategic mobility through increased airlift and sealift capabilities and prepositioned equipment.
- Reduce the time customers must wait for products and services.
- Fully implement total asset visibility across the Department.
- Reengineer and modernize existing logistics systems and processes.
- Minimize logistics costs.

Many ongoing logistics reform initiatives are focused on problems identified in previous audit and inspection reports, but it is imperative that a robust oversight effort continue in this area. Logistics reforms are generally interrelated with changes in acquisition or finance practices. It is particularly hard to implement process changes that cut across DoD organizations and “communities.” Also, most logistics improvements

“It is particularly hard to implement process changes that cut across DoD organizations and ‘communities.’”

depend on the successful introduction of new information systems. Because nearly all logistics operations lend themselves well to performance measurement, the progress and impact of the reform efforts, both individually and collectively, should be readily apparent. However, the DoD has much work to do to achieve reliable and timely performance reporting at the level of detail needed to fine tune logistics practices. Finally, infrastructure includes at least three areas where the risk of fraud is especially high—property disposal, health care and environmental cleanup.

During the reporting period, DoD auditors issued 41 reports on construction, other facilities issues, environmental programs, health care, supply and maintenance. Investigative efforts are discussed in Chapter Two.

INFORMATION TECHNOLOGY

Success in modernizing, improving effectiveness and reducing cost in all DoD management areas depends on overcoming information technology management challenges. The most formidable of the known challenges relate to ensuring the security of networked systems and overcoming a legacy of overly decentralized and poorly controlled information systems management, including ineffective oversight of major investment

“Success in modernizing, improving effectiveness and reducing cost in all DoD management areas depends on overcoming information technology management challenges.”

decisions. Issues related to the DoD information technology workforce may constitute an additional major challenge, but there is insufficient data available for determining the severity of the problems. Although outsourcing is often an effective alternative, this is not always the case.

The Y2K computing problem posed a huge challenge in terms of its scope, because all 10,000 DoD networks and 2.5 million computers were potentially affected. Likewise, the Y2K issue cut across DoD organizational and functional lines, involving warfighters and managers in all areas, not just information technology. The Y2K conversion effort was particularly difficult because the Department had seldom, if ever, been confronted by such an ubiquitous problem. The Department was also hampered by previous practices, such as lax configuration management, poor software documentation and inattention to contingency plans.

Despite those difficulties, the DoD Y2K effort was extremely successful. Only a few system failures occurred, operational impact was insignificant and surprisingly few problems occurred in supply chains and infrastructure, both in the United States and abroad. This does not mean that the Y2K problem was not real. The numerous findings in over 200 reports issued on Y2K conversion, as well as the hundreds of corrective actions taken in response to those reports, identified many risks that the Department ultimately was able to minimize. Those reports, which reflect the largest internal audit effort on a single subject in DoD history, also

...“One of the major success factors for DoD on Y2K was the transparency resulting from including Congress, General Accounting Office (GAO), OMB and the OIG, DoD, in all aspects of the DoD Y2K effort.”

demonstrate the powerful synergism that can be achieved between oversight organizations and program managers, without compromising the objectivity of either entity.

In the March 2000 report to Congressional defense committees on *Year 2000 (Y2K) Lessons Learned*, the Chief Information Officer, DoD, stated that “One of the major success factors for DoD on Y2K was the transparency resulting from including Congress, General Accounting Office (GAO), OMB and the OIG, DoD, in all aspects of the DoD Y2K effort.” We agree with this assessment and intend for the DoD internal oversight organizations to be extensively involved in the Department’s other information technology program efforts, especially security and system project management.

During this semiannual period, DoD auditors issued 35 reports on information technology issues. The heavy focus on Y2K conversion, however, necessitated scant coverage of other areas. Of the 29 OIG, DoD, information technology reports, 27 addressed Y2K issues, one concerned security and one addressed system project funding. Of the six Military Department audit reports, one was a Y2K summary and three related to security. With completion of the Y2K conversion, the oversight community needs to provide more coverage of other information technology issues. This is a high priority in our current planning, and we are working with the Department, GAO and interested Congressional committees to determine the specific programs and issues where audit coverage can be most useful. Senior OIG, DoD, and Chief Information Office, DoD, personnel have agreed to meet at least monthly on audit results and management plans related to system acquisition oversight.

Oversight activity on Information Assurance is discussed below as a Special Emphasis Area.

INFORMATION ASSURANCE

“...The DoD could not function successfully if its information systems were compromised or made to fail.”

Just as the human body cannot operate without its central nervous system, the DoD could not function successfully if its information systems were compromised or made to fail. Likewise, there are serious national security implications in vulnerabilities of non-military infrastructure, such as air traffic control systems or power distribution systems, to computer terrorism or cyberwarfare. The knowledge garnered over the past 3 years from another challenge to those systems, the “Y2K Bug,” will be invaluable in understanding the gravity of the information assurance problem and how to organize an effective program in response.

A massive effort was needed to solve the DoD Y2K conversion problem. The Department spent over \$3.6 billion, assessed more than 10,000 networked systems, conducted 88 multisystem end-to-end tests and 35 operational evaluation exercises, and coordinated with 5,000 critical suppliers, dozens of other agencies, host countries abroad and other allies on Y2K preparedness measures. Both the sheer magnitude of the effort and the information generated on DoD system inventories, interfaces, configurations and criticality underscore very graphically the dependence of military operations and DoD internal business functions on information technology systems.

In March 2000, the DoD provided a report to the Congress entitled *Year 2000 Lessons Learned* in response to a provision in the Defense Appropriations Act for Fiscal Year 2000. The report addressed Y2K lessons learned in the general context of improved management of cross-cutting information technology issues. Information assurance implications were not highlighted. Nevertheless, we agree with the insights provided by the report and believe that all of them are applicable in the information assurance effort.

The Y2K lessons discussed in the DoD report include:

- **Widespread applicability.** Overcoming an information technology problem as hard as the Y2K conversion was a significant confidence builder as the DoD faces other major information technology management issues.
- **Partnership.** Close cooperation between DoD and its suppliers, other agencies and other governments was vital.

- ***Focus on readiness.*** Managers and commanders will strongly support information technology efforts if there are clearly understood readiness effects. Without their involvement, the information technology managers cannot solve cross-cutting problems that impact operations.
- ***Horizontal problems require special management approaches.*** The DoD is organized along vertical lines. Cross-cutting problems require a team oriented approach and close Chief Executive Officer oversight to successfully resolve key organizational problems where responsibility does not lie solely with one major organizational component. The Y2K problem also showed the need for standardized guidance and performance measurement tools to focus efforts across the organization, coupled with proactive auditing and effective management response.
- ***Systems inventory visibility.*** The DoD must retain accurate and updated information on its systems, applying the data for information assurance status reporting and other management control purposes.
- ***Operational evaluations.*** The warfighting context provided by combatant command operational evaluations was critical to the DoD Y2K success. The operational evaluations validated information technology testing and evaluation, including examination of contingency plans. In the future, the Department will incorporate information assurance, critical infrastructure protection, interoperability and configuration management issues into routine Joint Staff, Combatant Command and Military Department exercise and training programs.

RECENT AUDIT AND INSPECTION RESULTS

The DoD audit organizations, as well as the Service Inspector General offices, produced over 200 reports on the Y2K conversion, leaving relatively few resources for information assurance coverage. Nevertheless, more than 20 reports were issued on the subject between January 1999 and March 2000. Those reports, which covered mostly the Army, Air Force and some Defense agencies, pointed out the need for a well-structured program with clear policies and metrics, as well as more aggressive measures to deal with chronic laxity in basic security procedures. The findings can be grouped into five problem areas.

First, pervasive problems exist in controlling access to databases and systems. The OIG, DoD, reported in December 1999 that DoD policy covering access controls over information systems had not been updated since March 1988 and had not kept pace with changing information infrastructure and technology advancements. Service, Defense agencies and Office of the Secretary of Defense policies governing the use of identification and authentication as a means of controlling access to information systems vary significantly. Until the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) updates information security policies or issues other policy guidance that specifically establishes uniform security requirements, DoD efforts to reduce vulnerability of the Defense Information Infrastructure will be hampered. In addition, reviews at DoD components such as the Army, Air Force, DFAS and Defense Information Systems Agency (DISA) identified numerous local access control issues.

Second, there has been mixed compliance with DoD requirements for system certification and accreditation. Accreditation is the formal declaration by the Designated Approving Authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation of an information system should be supported by a certification plan approved by the Designated Approving Authority, a risk analysis of the information system in its operational environment, a security safeguard evaluation and a certification report. Several reports identified DoD systems with incomplete certification and accreditation. Systems that are not properly certified and accredited are more vulnerable to attack.

Third, it is important to focus attention and resources on high risk areas, because the large number of DoD systems and organizations could quickly overwhelm an unprioritized information assurance effort. Many DoD component risk assessment programs are incomplete or ineffective.

Fourth, information assurance training needs more emphasis. The DoD Directive 5200.28 requires all persons accessing an automated information system to have completed a security training and awareness program. Although several of the audited DoD systems had security training and awareness programs in place, incomplete guidance, documentation and oversight resulted in users not receiving adequate training before they were granted access to sensitive computer systems, data and programs.

Fifth, despite heavy emphasis on system contingency plans and organizational business continuity plans during the Y2K conversion, many DoD managers regard updating contingency plans as a relatively low priority. The DoD Directive 5200.28 requires that contingency plans be developed and tested to ensure that automated information system security controls function reliably and that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. Procedures must be in place to recover data if it is modified or destroyed. We continue to find deficiencies in recovery plans, frequency of data back-up and testing.

FUTURE ACTIVITY

In testimony to the House Budget Committee in February 2000, the Deputy Inspector General, DoD, discussed these findings and concluded that DoD needs to:

- Adapt lessons learned from the Y2K conversion effort.
- Consolidate and update policy guidance.
- Establish better management control over the many separate efforts now under way or planned.
- Develop reasonable program performance measures.
- Ensure full attention to information assurance concerns in new system development and electronic commerce initiatives.
- Intensify on-site information security inspection and audit efforts.
- Improve training across the board for technical personnel, security officers and systems users.

The DoD is turning increased attention to these matters, but a sustained effort will be needed for the foreseeable future. To succeed, the Department will need robust audit, inspection and investigative support. The OIG, DoD, has assured DoD senior managers that a Y2K-like informal partnership with the Chief Information Officer on information assurance is both feasible and planned, although the audit resources earmarked for this matter will be far fewer than was the case for the extraordinary Y2K effort, due to budget constraints. We anticipate that managers and commanders at various levels will continue to want Service audit and inspection coverage as well.

The DoD criminal investigative community is focused on computer crimes, which range from child pornography and Web page defacements to denial of service, root intrusions, theft of critical technology and virus attacks. Computer crime investigations require specialization regarding the investigation, seizure and forensic analysis of information. This has caused the reallocation of limited resources, including manpower and funding to cover the costs of training and updated specialized investigative equipment.

To meet the challenges in this area, the Department established the DoD Computer Forensics Laboratory and the DoD Computer Investigations Training Program. The DoD also set up the Joint Task Force-Computer Network Defense (JTF-CND) with responsibility, in conjunction with the Combatant Commands, Services and Defense agencies, for coordinating and directing the defense of DoD computer systems and computer networks. The Law Enforcement/Counterintelligence Cell (LE/CIC) operates within the JTF-CND to coordinate DoD law enforcement and counterintelligence investigations. All defense criminal investigative organizations are represented within the LE/CIC. In addition to coordinating within the DoD, the LE/CIC is also in direct communication with the National Infrastructure Protection Center.

Computer crime investigative units have been established in each of the defense criminal investigative organizations to combat computer intrusions into the DoD information infrastructure and to seize and analyze computer crime evidence.

The intelligence community has also had a longstanding role in information assurance. The Intelligence Community Inspector General Forum established the Information Assurance Working Group in September 1999. The objective of the Working Group is to enhance management of information assurance throughout the intelligence community through information sharing and coordination and by appropriate individual and joint projects that assure the accountability, availability, integrity, authenticity, confidentiality and non-repudiation of information services. Further discussion of information assurance oversight in the intelligence community is included in the Classified Annex to this report.

POLICY STILL EVOLVING

Federal information assurance policy continues to develop. The Congress and the OMB are considering additional guidelines that would affect future DoD efforts. Specifically, S.1993, the Computer Security Improvement Act of 1999, would mandate a strong OMB role and require annual evaluations of each department's information security posture. In the case

of systems used to support national security missions, the Secretary of Defense and Director of Central Intelligence would determine independent evaluation mechanisms and the Inspectors General of the DoD and Central Intelligence Agency would audit the respective evaluations of their Department or Agency. The OIG, DoD, has commented favorably on S.1993. The Bill's emphasis on continuous risk management is well placed, and the requirement for annual security posture evaluations, validated by audits, is reasonable.

The OMB is staffing proposed revisions to Circular A-130, Management of Federal Information Resources, which also would strengthen the OMB role in information assurance oversight. The DoD is unlikely to welcome detailed OMB reporting requirements; however, the OIG, DoD, believes that OMB needs to have an active oversight role in this area and meaningful oversight is impossible without current, reliable and sufficiently detailed information. We recommend that the DoD and OMB share the same management information data set, which will be classified.

The OIG, DoD, and GAO have reported several times that DoD information security policies need to be updated, consolidated and clarified. Efforts are under way to do so. It is important, of course, that additional Congressional and OMB requirements be accommodated in the ongoing policy revisions.

SUMMARY

The DoD has been accelerating its information assurance efforts over the past several years, regardless of the Y2K distraction. In fact, the Y2K effort provided many useful insights and lessons to be applied as the Federal and DoD information assurance programs develop. This will remain a high risk area for the indefinite future and merits very close attention from senior managers and the Congress.

CHAPTER TWO - SIGNIFICANT ACTIVITIES

INTRODUCTION

This chapter summarizes the significant activities of the OIG, DoD, components and their work with other members of the DoD oversight community.

CRIMINAL INVESTIGATIONS

The four Defense Criminal Investigative Organizations (DCIOs) continue to combat crime affecting the DoD and the Military Departments. The Defense Criminal Investigative Service (DCIS), the criminal investigative arm of the OIG, DoD, focuses the bulk of its 321 civilian criminal investigators on the investigation of procurement fraud by Defense contractors and health care fraud by health care providers. The Army Criminal Investigation Command (CIDC), the Naval Criminal Investigative Service (NCIS) and the Air Force Office of Special Investigations (AFOSI), also investigate procurement fraud, but focus the majority of their resources on other crimes against persons and property affecting their respective Military Departments. The AFOSI and NCIS also conduct counterintelligence investigations and operations. This section focuses on the procurement, health care and other major fraud investigations accomplished by the DCIOs.

Figure 1 (page 14) displays the investigative results achieved by the four organizations during this period. As in previous reports, the statistics do not include general crime investigations (other than large-scale thefts) or counterintelligence activities.

Examples of Major Procurement Fraud

The following are examples of some of the more significant fraud cases investigated by the DCIOs during this semiannual period. It should be noted that in virtually all instances, the Defense Contract Audit Agency (DCAA) played a critical role in supplying needed audit support.

Alliant Techsystems, Incorporated, agreed to pay \$1,316,532 in civil restitution to settle allegations that it failed to provide Army contract negotiators with the most current, complete and accurate cost and pricing data for the purchase of AT-4 Light Anti-Armor Weapons. The complaint alleged that negotiators were not notified that Alliant was changing from a two- to a one-piece muzzle cover, which should have resulted in a substantial reduction in cost to the Government.

David M. Mitchell, co-owner and president of Campbell M. Industries, Incorporated, was initially investigated for product substitution, for which he was tried, convicted and sentenced. While being investigated for the

DEFENSE CRIMINAL INVESTIGATIVE ORGANIZATIONS CASE RESULTS			
	Procurement Fraud and Major Health Care Fraud Investigative Case Results	Other Criminal Investigative Results	Total
LITIGATION RESULTS			
Indictments - DoJ	82	118	200
Convictions - DoJ	81	112	193
Indictments - State/Local/Foreign	7	42	49
Convictions - State/Local/Foreign	1	44	45
MONETARY OUTCOMES			
DoJ Only	\$484,907,633	\$13,213,419	\$498,121,052
DoD Administrative Recoveries	20,764,401	290,216	21,054,617
DoD Investigative Recoveries	665,783	12,315,249	12,981,032
State/Local/Foreign	13,147	432,363	445,510
Total Monetary Outcomes	\$506,350,964	\$26,251,247	\$532,602,211
SUSPENSIONS AND DEBARMENTS RESULTING FROM INVESTIGATIONS			
Suspensions			
Individual	21		
Companies	21		
Debarments			
Individual	32		
Companies	16		

Figure 1



E8-C Joint Surveillance Target Attack Radar System (JSTARS) Aircraft

first matter, Mitchell attempted to negotiate a stolen U.S. Treasury check by falsely representing the check as payment for DoD contract work he had performed. As a result of this separate violation, Mitchell was arrested, pled guilty to bank fraud and sentenced to 33 months confinement, 5 years probation and ordered to pay \$197,717 in restitution.

Northrop Grumman agreed to pay a \$750,000 civil settlement to the Government to resolve issues of substandard work. Northrop Grumman's Louisiana Corporation was investigated for allegedly failing to properly calibrate ovens used to heat-treat aluminum aircraft parts used on the E8-C Joint Surveillance Target Attack Radar System (JSTARS) Aircraft, among other improper practices. Two individuals who filed a related *qui tam* complaint will share \$180,000 of the settlement amount.

Page AvJet Corporation (PAC) agreed to pay a \$1.395 million civil settlement to resolve false claims issues regarding U.S. Foreign Military Funding (FMF) granted to the Government of Israel. Under FMF rules, administered by the Defense Security Assistance Agency, PAC certified that over half of the value of goods and services it provided to Israel was of American origin. However, results of the investigation indicated that most of the work was performed by an Israeli contractor in Israel.

Examples of Health Care Fraud

“...eight hospitals and medical centers agreed to pay a total of \$1,121,480 in civil restitution....”

An investigative project identified 18 hospital laboratories engaged in improper/illegal billing practices. The scheme involved unbundling chemical profiles and billing for them separately, resulting in excessive or duplicate charges paid by the TRICARE (the health care system for uniformed Service members and their dependents), Medicare, Medicaid and various insurance companies. During the current reporting period, eight hospitals and medical centers agreed to pay a total of \$1,121,480 in civil restitution to the Government to resolve these issues.

John R. O'Donnell, M.D., was investigated for defrauding Blue Cross-Blue Shield, Medicare and TRICARE through various improper billing schemes and billing for procedures he was not authorized to perform as a general practitioner. Following indictment, he and his wife were arrested for violating conditions of their pre-trial release. They allegedly took the assets from the sale of properties that had been used as securities for their release and placed them in “offshore accounts” while preparing to flee the United States. O'Donnell was convicted of mail fraud, tax evasion, money laundering and illegal distribution of a controlled substance. He was ordered to forfeit the properties obtained through his illegal conduct, plus his retirement account, a total value of approximately \$553,000; he awaits sentencing. Carol O'Donnell, who worked in her husband's medical office, pled guilty to mail fraud for submitting false billing documents to insurers. She was sentenced to 21 months in prison, 3 years supervised release and ordered to pay \$688,278 in restitution.

“A \$486 million global settlement was reached with Fresenius Medical Care headquartered in Lexington, Massachusetts. The settlement is the result of a 5-year, multi-agency investigation....”

A \$486 million global settlement was reached with Fresenius Medical Care headquartered in Lexington, Massachusetts. The settlement was the result of a 5-year, multi-agency investigation into allegations that National Medical Care (NMC) conspired to defraud the United States through the submission of false claims and the payment of kickbacks. The NMC, purchased by Fresenius in 1996, provided services and supplies for patients with end-stage renal disease. The alleged false claims included billing unnecessary

laboratory tests and nutritional services, falsifying documents and double billing laboratory services. As part of the settlement, three NMC divisions—NMC Homecare Division, Lifechem Laboratory and Medical Products Division—each pled guilty to conspiracy to defraud the United States. Former company officials pled guilty and await sentencing or have been indicted and await trial.



Psychiatrist Kristopher K. Wendler was convicted in 1995 on a 15-count criminal information for fraud. A follow-on investigation found evidence that for 5 years Wendler defrauded TRICARE, Medicare and Medicaid, and, although licensed to practice in Kansas, he operated without a license in Missouri. His license was suspended in October 1997. Wendler allegedly defrauded TRICARE through such schemes as billing for 40 individual therapy sessions when he actually provided group therapy, billing for much longer sessions than he provided and billing for services he was not licensed to perform. Wendler was arrested in January 1998 and indicted on the current charges. He was denied parole on his state fraud charges in 1999 since he was considered to be a threat to witnesses who testified against him and a flight risk in light of the potentially lengthy jail time he faced. A Federal trial jury found Wendler guilty of 21 counts of mail fraud. He was sentenced to 46 months imprisonment, 3 years probation and ordered to pay \$206,688 restitution and a \$2,100 special assessment.

“...a divisional chief executive officer...was sentenced to 33 months in prison, 3 years probation and ordered to pay a \$10,000 fine and \$1,683,417 in restitution.”

An investigation of Columbia Healthcare Corporation for fraud against TRICARE, Medicare and Medicaid found evidence that two of the corporation’s executives filed fraudulent cost reports since 1987 for Columbia’s Fawcett Memorial Hospital in Florida. Both executives were convicted in a jury trial of false statements, conspiracy and fraud. Robert Whiteside, Director of

Reimbursement, was sentenced to 24 months in prison, 3 years probation and ordered to pay a \$7,500 fine and \$645,796 in restitution. Jay Jarrell, a divisional chief executive officer, was sentenced to 33 months in prison, 3 years probation and ordered to pay a \$10,000 fine and \$1,683,417 in restitution.

A *qui tam* complaint alleged that the University of Chicago Hospital and the physicians assigned to the Hematology/Oncology Clinic billed Medicare and Medicaid, against regulations, for the services of an attending physician when the services were actually performed by a resident physician and conspired to conceal that activity. Additional allegations, which also affected TRICARE, included billing for complex

examinations regardless of the services rendered, and billing for consultations even though it was not the patient's first visit to the clinic doctor. To resolve these allegations, the hospital agreed to pay a total of \$10,900,000 in civil restitution to the Government and the State of Illinois. The relator will receive \$1.85 million of this settlement.

Other Criminal Investigative Results

In addition to the matters listed above, the DCIOs conducted various other significant investigations involving large-scale thefts and non-procurement related fraud.

Marketing Fraud

"American Fidelity Life Insurance Company...and Trans World Assurance Company...agreed to pay \$10,109,303 in administrative settlements...."

American Fidelity Life Insurance Company (AFLIC) and Trans World Assurance Company (TWAC) agreed to pay \$10,109,303 in administrative settlements to resolve a variety of alleged violations. The companies primarily targeted financially inexperienced soldiers, sailors, marines and airmen in an effort to sell them life insurance policies allegedly misrepresented as "investments," "savings plans" and "retirement plans." Some sales agents were retired military members who entered military installations using their retired military ID cards. To gain access to young, unsuspecting military members, sales agents allegedly bribed some noncommissioned officers or convinced others that their product was "good" for Service members. Sales agents allegedly used a variety of fraudulent sales pitches, such as claiming that the life insurance plan officially available through the DoD (Servicemen's Group Life Insurance (SGLI)) would not cover the Service members in non-combat areas or when they were off duty, which caused some Service members to cancel their SGLI enrollment. Another misleading ploy was claiming that Service members could not secure a Department of Veterans Affairs loan unless they were in a retirement plan with AFLIC or TWAC. More than \$7.7 million of the settlement will be refunded to Service members who invested in AFLIC or TWAC products between 1977 and 1997. The agreement also specified a mechanism for other Service members to seek refunds, as well as a corrective action and an oversight plan.

False Claims

A multi-agency investigation of a *qui tam* complaint resulted in significant civil settlements with three entities. To resolve allegations of false claims against Medicare, Medicaid, TRICARE and the Federal Employees Health Benefits Program, Medical Consultants, Incorporated (doing business as Emergency Physicians Billing Service), and its president, Joseph D. McKean, M.D., agreed to pay a total of \$15 million in restitution. The relator will receive \$1 million directly from the defendants, plus 25 percent of the Government's share; more than \$2

million will go to the affected states. In a separate civil settlement, affiliate MBLs Emergency Physicians agreed to pay a total of \$87,000 in restitution to the U.S. Government and the State of Florida. The companies allegedly engaged in upcoding, billing for services not performed and billing twice for the same procedure.

An investigation found evidence that, although suspended and debarred from conducting business with the DoD, Robert Silver, former president of Silver Sales, Incorporated, submitted numerous false claims to the Defense Supply Center, Richmond, Virginia (DSCR). The claims misrepresented the manufacturer and quality of chemical products supplied on DCSR contracts for use by NASA and the DoD. Silver pled guilty to one count of false claims to a Federal agency and was sentenced to 33 months imprisonment, 3 years probation and ordered to pay restitution of \$148,089.

Diverse Technologies Corporation (DTC) and its president agreed to pay a \$400,000 settlement to resolve false claims allegations. The DTC is alleged to have knowingly billed the Navy for hours worked by DTC employees who were not qualified for the labor categories under which they were billed, and billed the Navy for work by DTC employees not chargeable to Government contracts. The DTC provided management and technical support to the Navy for consolidation of its accounting systems.

Occupational Training, Incorporated (OTI), and its president, Marcus Bass, agreed to pay a civil settlement of \$97,376 to resolve false claims allegations. The OTI provided Asbestos Hazard Emergency Response Act (AHERA) training to military units in Hawaii and Japan. Bass claimed he was accredited by the State of Indiana, an EPA licensed state, to conduct AHERA training. The investigation found evidence that Bass presented 14 AHERA classes without possessing the proper accreditation.

Environment

American Processing Company, National City, California, entered into a settlement in the Southern District of California Federal Court whereby the company agreed to pay civil fines of \$3,000,000 for the transportation of 135 tons of hazardous waste without a uniform hazardous waste manifest. American Processing Company was subcontracted to dispose of “organo” lead contaminated soil from a construction site at the Naval Amphibious Base, Coronado, California.

Export Control Violations

Orbit/FR, Incorporated (Orbit), a DoD contractor located in Pennsylvania, pled guilty to two counts of violating the Arms Export Control Act and was fined \$600,000. The investigation found evidence that Orbit exported



Patriot Missile

defense articles and services, through its parent company in Israel, to the People's Republic of China without proper licenses or authorization from the Departments of State or Commerce. This included military equipment for use in China's missile development program that had been developed for the Israeli Defense Forces. Orbit also provided technical expertise to improve the accuracy of a Chinese surface-to-air missile system similar to the Patriot missile system.

Contracting Fraud

Gothrie Short, President of Tri Gems Builders, and Jason Griffin, Vice President, were convicted and sentenced in New Jersey for their role in conspiring to fraudulently obtain U.S. Government contracts awarded under the Small Business Administration's Set-Aside Program on a non-competitive basis and inflating costs associated with those contracts. Both were sentenced to 3 years probation and ordered to pay a \$10,000 fine and restitution in the amount of \$315,000.

Jacobs Engineering Group, Incorporated, sold its corporate headquarters in Pasadena, California, under a sale/leaseback arrangement with the Government, but allegedly continued to charge the Government a higher price to offset its overhead costs in violation of Federal Acquisition Regulations. Jacobs Engineering subsequently agreed to a global settlement of \$35,000,000 in return for a stipulation of dismissal of charges.

Kickbacks/Bribery

A 4-year undercover investigation into the maritime industry identified widespread corruption in the repair and maintenance of Government ships in the DoD Military Sealift Command (MSC) fleet and the Department of Transportation (DOT) Maritime Administration (MARAD) fleet. As of March 2000, there were 43 indictments against 31 individuals and companies. The following paragraphs illustrate some of the results.

Warren Hilton, a surveyor for the MARAD in Beaumont, Texas, pled guilty to bribery. Hilton received merchandise from CBH Services, a MARAD contractor, including a large screen television, video cassette recorder, power washer, computer and more, with a total value of more than \$16,000. The costs of these items were then concealed in false invoices submitted by CBH to the Government. Hilton was sentenced to 4 months in prison, 4 months home detention and ordered to pay \$7,460 in restitution.



USNS Denebola (T-AKR 289)
Fast Sealift Ship

Janco Ship Repair, Incorporated, and its owner, Joseph LeClair III, pled guilty to paying kickbacks to port engineers in return for favorable treatment. Janco was sentenced to a \$1,550 fine and \$200 special assessment. In both Florida and Virginia, LeClair received concurrent sentences of 3 years probation, including 6 months home detention, and was ordered to pay a total fine of \$3,000. Janco, a subcontractor to Bay Ship Management, Incorporated, performed repairs aboard MSC ships. Bay Ship held multi-million dollar prime contracts with the Navy to oversee the operation and repair of Navy vessels.

Joseph Wing, a former DOT MARAD employee, introduced Boston Ship Repair (BSR) officials to a Bay Ship official. In return for the introduction, BSR paid Wing a “consultants fee” that he did not claim on his income tax return. Wing pled guilty and was sentenced to 2 years probation and ordered to pay a \$2,000 fine for income tax evasion.

For violating the anti-kickback statute, BSR’s president and vice president were each sentenced to 12 months incarceration, 2 years probation and ordered to pay a \$30,000 fine. Investigation found that the two BSR executives paid kickbacks to an official of Bay Ship in return for ship repair subcontracts.

“Five individuals pled guilty to paying or receiving kickbacks and were sentenced to imprisonment and/or probation.”

Investigation revealed alleged kickbacks paid by subcontractors to obtain ship repair contracts from two master ship repair companies (MSRs). Five individuals pled guilty to paying or receiving kickbacks and were sentenced to imprisonment and/or probation. Three companies, Gamma Tech Industries, Tidelands Testing and San Diego Marine Piping, pled guilty to paying kickbacks and were each sentenced to 5 years probation. The companies and two of the individuals will pay a total of \$1,513,741 in joint or separate restitution to the United States and to one of the MSRs.

Donna LeMaire, President of Triplex Marine Maintenance Incorporated, Port Arthur, Texas, and Keith Courvelle, a Triplex superintendent, pled guilty to paying kickbacks. Danny Weldon, a Triplex estimator, pled guilty to theft of Government funds. LeMaire, Courvelle and Weldon were each sentenced to 3 years probation, including 3 months home detention, and ordered to share in paying \$67,185 in restitution. LeMaire and Courvelle were fined \$10,000 each; Weldon was fined \$5,000. The

investigation found that LeMaire and Courvelle paid kickbacks in the form of secretarial services, entertainment and travel expenses and other gratuities to port engineers employed by Bay Ship in New Orleans. The kickbacks, which ensured favorable treatment (subcontract awards) by Bay Ship, were reimbursed through falsified invoices charged to the MSC.

Theft/Forgery

Two checks intended as payment to a DoD contractor were negotiated after being reported missing. Investigators tracked one \$12,600 check to a liquor establishment that cashed the check for a regular customer. Robert Stanton, who confessed to finding the checks in a trash bin located near the DoD contractor's former address, voluntarily turned over the \$15,000 in cash remaining from the original \$75,000 in checks. Stanton pled guilty to forgery and was sentenced to 5 years probation, including 6 months home confinement with electronic monitoring, and ordered to pay \$60,000 in restitution.

HOTLINE



During this reporting period, the Hotline received 6,245 telephone calls, letters and electronic mail resulting in the initiation of 1,263 cases. During the same period, the Hotline closed 1,039 cases. The Hotline responded to 126 requests for posters and other marketing material from DoD activities and DoD contractors in our continuing effort to identify fraud and waste within the DoD. Since 1982, over \$419 million has been recovered as a direct result of inquiries initiated in response to information provided to the Hotline.

Significant Hotline Complaints

As a result of a Hotline complaint, a subsequent DCIS and NCIS investigation substantiated allegations that Hughes Aircraft of Mississippi, Incorporated, intentionally installed substandard and untested components in "ADCAP Mk 48" torpedoes. Negotiations with General Motors, the parent company, led to a settlement of \$500,000.

As a result of an anonymous Hotline complaint, the U.S. Army Criminal Investigation Division conducted an investigation into allegations that Allied Signal submitted fraudulent billings to the Government. Without any admission of liability or fault, the contractor entered into a civil settlement and agreed to pay \$200,000 to the U.S. Treasury.

ADMINISTRATIVE INVESTIGATIONS

The OIG, DoD, Departmental Inquiries Office conducts investigations and also performs oversight of investigations conducted by the Military Departments. These investigations pertain to:

- Allegations of reprisal against military members, Defense contractor employees and nonappropriated fund employees.
- Allegations that military members were referred for mental health evaluations without being afforded the rights prescribed in the DoD Directive and Instruction pertaining to mental health evaluations of members of the armed forces.
- Noncriminal allegations against senior military and civilian officials.

Whistleblower Reprisal Activity

During the reporting period, the Special Inquiries Directorate and the Inspectors General of the Military Departments received 185 complaints of whistleblower reprisal. We closed 142 cases during this period. Of those, 100 were closed after preliminary analysis determined further investigation was not warranted, and 42 were closed after full investigation. Of the 42 cases closed after full investigation, eight (19 percent) contained one or more substantiated allegations of whistleblower reprisal.

Referrals for Mental Health Evaluations

Thirteen cases closed during the reporting period contained allegations of improper referrals for mental health evaluations. We did not substantiate that any mental health evaluation referrals were used to reprise against Service members for whistleblowing. However, we concluded that in five of the 13 cases, commanders failed to follow the proper procedures for referring a Service member for a mental health evaluation under DoD Directive 6490.1, "Mental Health Evaluations of Members of the Armed Forces."

Figures 2 and 3 (page 23) show the types and distribution of whistleblower reprisal cases as of March 31, 2000.

Examples of Substantiated Military Whistleblower Reprisal Cases

An Army sergeant first class received counseling statements, a suspension of platoon sergeant duties, an initiation of a field grade administrative disciplinary action and an unfavorable (Relief for Cause) Noncommissioned Officer Evaluation Report in reprisal for making protected communications to his company commander. The sergeant first class had reported his perceptions of improper off-post conduct by an officer and two senior noncommissioned officers. The responsible management officials have retired or resigned their commissions.

An Air National Guard female staff sergeant received an unfavorable performance report in reprisal for making complaints of favoritism and sexual harassment against her supervisor, a senior master sergeant. The

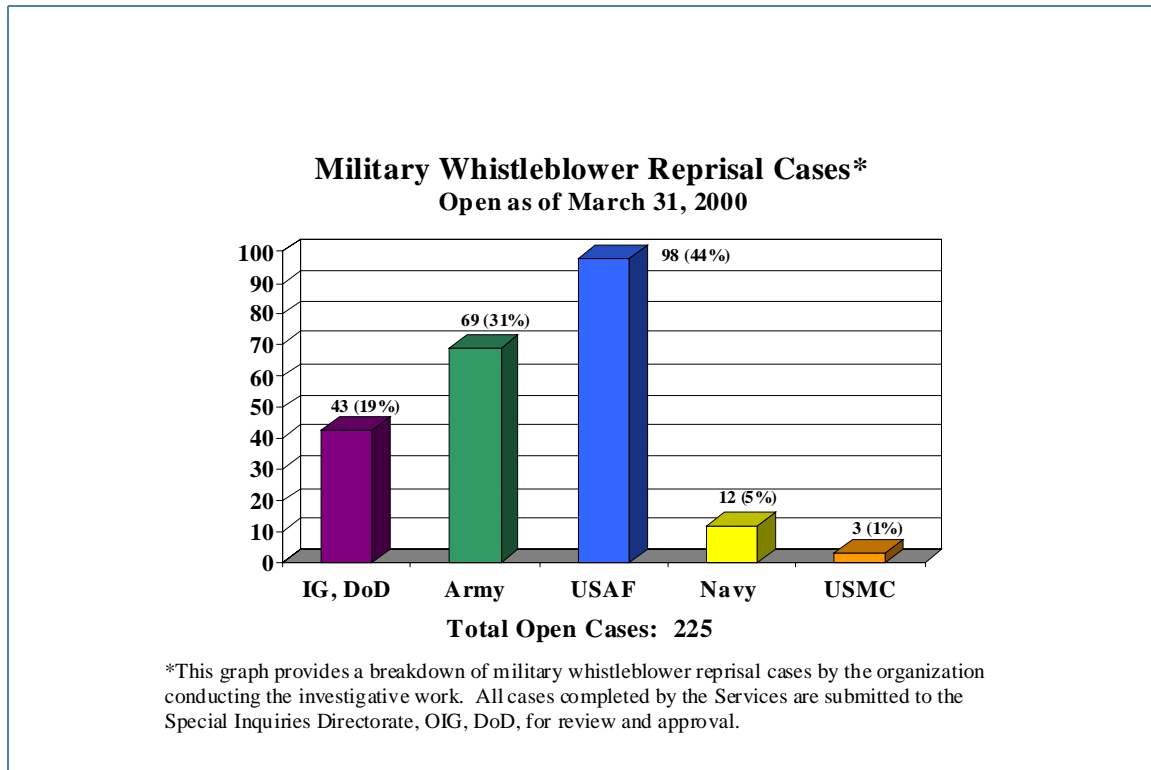


Figure 2

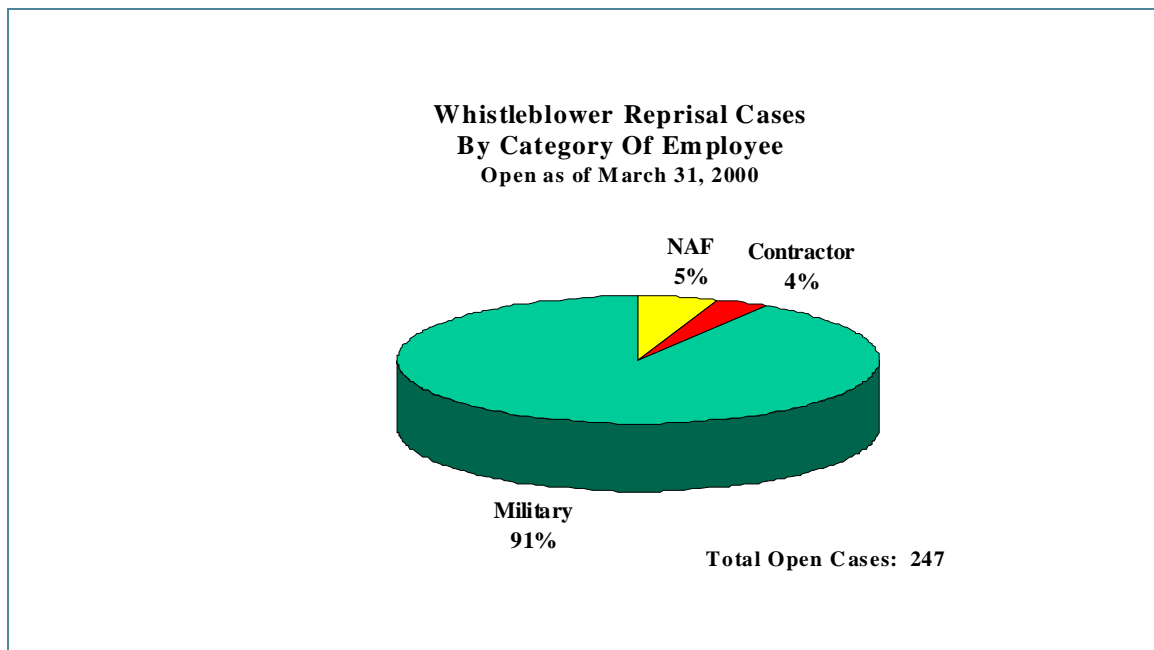


Figure 3

responsible management official received a letter of reprimand that will remain in his record for one year.

A Navy communications specialist first class received an unfavorable Evaluation Report and Counseling Record for filing two complaints with a Navy Inspector General and for filing an Article 138 complaint against his commanding officer. Corrective action is pending before the Navy.

Senior Official Inquiries

Figures 4 and 5 (page 25) show results of activity on senior official cases during the period. On March 31, 2000, there were 235 ongoing investigations into senior official misconduct throughout the Department, remaining nearly constant since October 1, 1999, when we reported 229 open investigations. Over the past 6 months, we closed 250 senior official cases, of which 30 (12 percent) contained substantiated allegations.

Examples of Cases Involving Senior Officials

We substantiated allegations that a senior DoD official misused his position by arranging official duties as a pretext for obtaining Government funded travel when the primary purpose of the travel was, in fact, personal business. Further, we found that on other occasions the senior official conducted travel at Government expense that served no substantial official purpose or was wasteful because the stated purpose of the travel was of incidental benefit to the Government. Finally, we found that the senior official violated DoD ethics regulations by allowing his

“...a senior DoD official misused his position by arranging official duties as a pretext for obtaining Government funded travel...”

subordinates to perform personal services for him in connection with official travel. The results of the investigation have been provided to the cognizant Military Department for consideration of corrective action.

At the request of a Member of Congress, we investigated allegations that a senior DoD official violated restrictions concerning a conflict of interest by taking official action in matters involving a company with whom he was pursuing post-retirement employment. The case was particularly noteworthy because the senior official allegedly used his position to influence the results of an aircraft accident review to benefit the defense contractor, which eventually employed him after he retired from Federal service. Although we confirmed that the senior DoD official participated in matters that involved the contractor with whom he later accepted post-retirement employment, we determined that his official actions did not have a "direct and predictable effect" on the financial interests of the contractor. As a result, we concluded that he did not violate applicable statutory or regulatory restrictions concerning a conflict of interest. The

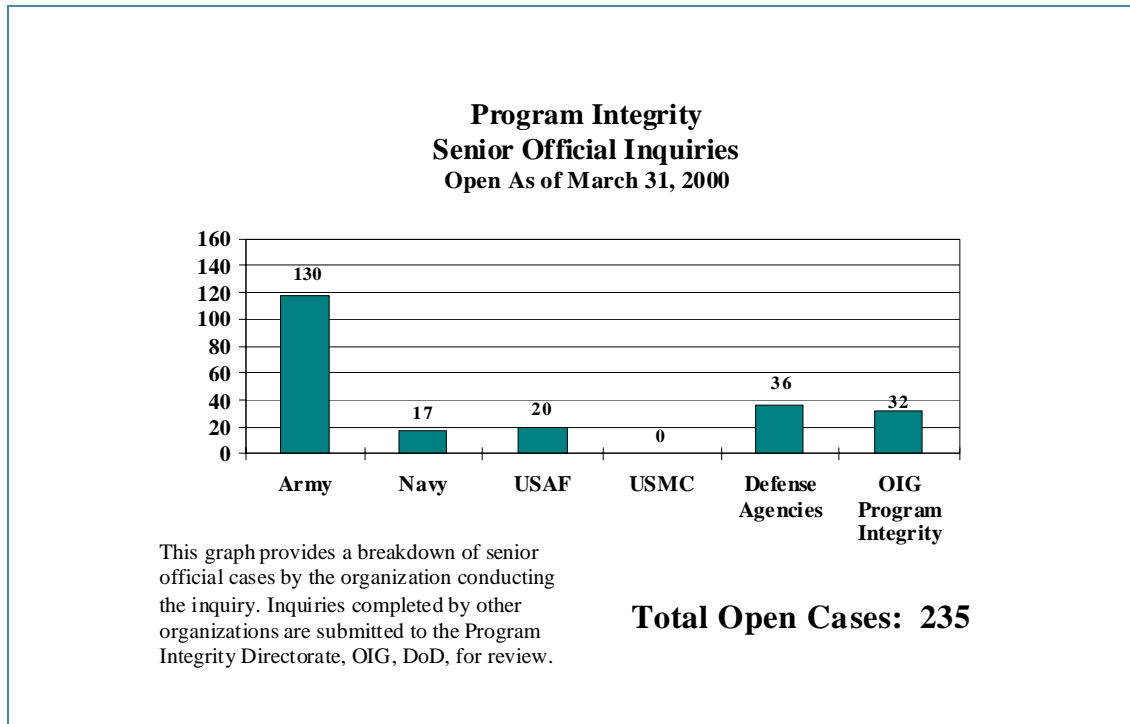


Figure 4

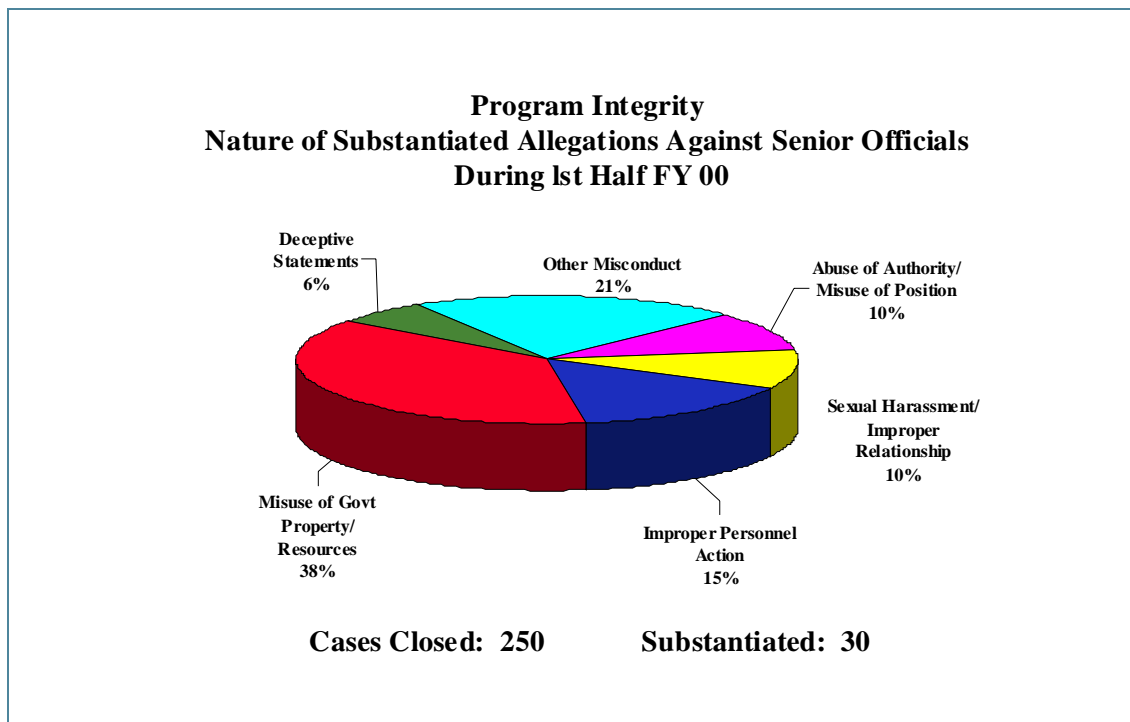


Figure 5

case illustrated the difficulty of applying conflict of interest prohibitions in certain situations.

CRIMINAL INVESTIGATIVE POLICY AND OVERSIGHT

The Office of Criminal Investigative Policy and Oversight (CIPO) published the following significant reports during the reporting period.

Our report, *Evaluation of the Criminal Investigative Environment in which the Defense Enrollment Eligibility Reporting System Operates*, evaluated the ability of DoD to prevent, detect and investigate health care beneficiary fraud. The report made six recommendations aimed primarily at reducing the number of ineligible persons availing themselves of military medical benefits and ensuring that upon detection those instances were properly recorded, referred to investigators and followed up. The report also sought to raise the awareness of the importance of this area of potential fraud by recommending greater management controls and vigilance.

In conjunction with the Office of the Assistant Inspector General for Auditing, an oversight review of the OIG, Defense Intelligence Agency (DIA), was conducted. For this review, CIPO assessed the management and effectiveness of the OIG, DIA, investigative program. The CIPO made nine specific recommendations to enhance the organization, mission, policies, procedures, training and staffing of this investigative program.

In addition to these reports, CIPO prepared and is administering the Deputy Secretary of Defense tasking to the Services to accomplish those recommendations of the National Academy of Public Administration's report, *Adapting Military Sex Crimes Investigations to Changing Times*, in which DoD concurred. The OIG, DoD, was designated to monitor the progress of the completion of these taskings on behalf of the Deputy Secretary of Defense.

Voluntary Disclosure Program

The DoD Voluntary Disclosure Program encourages contractors to disclose potential criminal or civil fraud that may affect their contractual relationship with the DoD or the contractor's responsibility under Federal Acquisition Regulations. The following are examples of voluntary disclosures that resulted in monetary payments to the Government during this reporting period.

The Aluminum Company of America (ALCOA) agreed to pay \$727,000 in damages and penalties after failing to consistently perform fracture toughness testing of extrusions required by contract specifications. In



C-17 Aircraft

some instances, no testing was done and in other instances, inadequate testing was conducted on parts used in C-17 aircraft.

Contract specifications required Hughes Aircraft Company to perform performance and acceptance tests on traveling wave tubes, components used in radar systems on F-14 and F-15 aircraft. Such testing was not accomplished on three different models of the tubes, and investigation also determined Hughes inflated labor hours billed to the Government. A settlement agreement was reached in the amount of \$2,113,000.

AUDITING

The OIG, DoD, and Military Departments' central audit organizations issued 181 reports during the reporting period, identifying \$1.2 billion in quantifiable monetary benefits and addressing a wide spectrum of DoD programs, with emphasis on the high risk areas discussed in Chapter 1. Appendix A lists internal audit reports by major subject area. Appendices B and C list OIG, DoD, reports with potential monetary benefits and summarize internal audit followup activity, respectively.

The DCAA continued providing a range of support to DoD contracting officers and questioned \$516.1 million in costs, as summarized in Appendix D.

Climate Assessment

At the request of the Secretary of Defense, the OIG, DoD, assessed the environment at 38 installations and on 11 ships regarding the application of the DoD homosexual conduct policy, which is commonly referred to as the "Don't Ask, Don't Tell" policy. The Secretary requested that the survey assess the extent to which:

- Harassment of Service members based on perceived homosexuality may occur.
- Disparaging speech or expression with respect to sexual orientation may occur.
- Such speech or expression may be tolerated.

To conduct the assessment, we surveyed nearly 72,000 active duty Service members, using random sampling to choose locations and units. For each selected unit, we administered a questionnaire to all unit

members. The questionnaires were designed and processed with emphasis on ensuring the anonymity of all respondents. Cooperation by the Defense Manpower Data Center and the Military Departments, especially unit commanders, was excellent.

“...80 percent of the respondents stated they had heard offensive speech, derogatory names, jokes or remarks about homosexuals in the last 12 months.”

Regarding the environment at the surveyed locations, 80 percent of the respondents stated they had heard offensive speech, derogatory names, jokes or remarks about homosexuals in the last 12 months. Eighty-five percent believed such comments were tolerated to some extent. Thirty-seven percent of the respondents stated that they had witnessed or experienced an event or behavior toward a Service member that they considered to be harassment based on perceived homosexuality. About 5 percent believed that harassment based on perceived homosexuality was tolerated by someone in their installation or ship chain of command, and 10 percent believed it was tolerated by other unit members. About 78 percent of the respondents indicated they would feel free to report harassment of perceived homosexuals. Overall, 97 percent of the respondents believed they had at least some understanding of the homosexual conduct policy. Approximately 57 percent of the respondents stated they had not had training on the policy. Finally, 50 percent of the respondents stated the policy was moderately or very effective at preventing or reducing harassment; 46 percent stated it was slightly or not effective; and 4 percent did not provide a response.

In February 2000, the Secretary of Defense approved Military Department training plans intended to emphasize that harassment of Service members for any reason, including perceived sexual orientation, is unacceptable. In addition, in response to the survey results, the Secretary formed a senior-level task force to develop recommendations for further corrective actions. The OIG, DoD, effort was particularly noteworthy in that the entire project, to include the development of the survey instrument, site visits, survey administration, analysis and report issuance was accomplished in a 90-day period as requested by the Secretary.

Export Licensing

The National Defense Authorization Act for Fiscal Year 2000 required that the Inspectors General of the Departments of Commerce, Defense, Energy and State conduct an annual review of the policies and procedures of the U.S. Government to prevent the export of sensitive technologies and technical information to countries of concern. This year's review focused on compliance with the “deemed” export licensing requirements contained in Export Administration Regulations and the International Traffic in Arms Regulations. Foreign nationals visit Federal research

facilities for a variety of reasons under various international agreements and programs. During these visits, they may have access to export-controlled software or technology. The release to foreign nationals of technical data that meet the criteria of the Export Administration Regulations or the International Traffic in Arms Regulations is considered an export. According to these regulations, the oral, visual or written disclosure of technical data to a foreign national may require a “deemed” export license.

“...DoD research facilities provided technical data to very large numbers of foreign visitors without determining whether an export license was required.”

All of the OIGs reported weaknesses in their agencies’ controls. The DoD research facilities did not have procedures for determining whether a deemed export license was required in conjunction with the disclosure or release of technical data to

foreign nationals. In addition, Military Department program officials were not knowledgeable of the term “deemed export” or of the licensing requirements for such exports. As a result, DoD research facilities provided technical data to very large numbers of foreign visitors without determining whether an export license was required. Also, DoD seldom provided proposed data exchange agreement annexes to the Department of Commerce for review. From 1994 through 1999, the Military Departments signed 316 data exchange agreement annexes; however, DoD provided only 48 to the Department of Commerce. As a result, DoD was not necessarily reflecting a U.S. Government consensus position when approving most data exchange agreement annexes. These results were included in an interagency report, a DoD-specific report and a classified report that is summarized in the Classified Annex to this report.

Auditor Independence

The Advisory Council on Government Auditing Standards is considering a proposal to adopt the American Institute of Certified Public Accountants definition of auditor independence. Because the Auditors General of the Military Departments are selected by their Department Secretaries and not a legislative body, and are not covered by the Inspector General Act, this change would call into question the ability of the Service audit organizations to provide independent opinions on Army, Navy and Air Force financial statements.

On February 22, 2000, the Deputy Inspector General, DoD, wrote to the Advisory Council urging that the many measures taken by the Congress, the Military Departments and the OIG, DoD, to assure the independence of the Army, Navy and Air Force audit organizations be recognized. To comply with the massive financial statement audit workload mandated by the Chief Financial Officers Act, the DoD internal audit community

“Forcing a diminished role for the Service auditors...could pose another significant and unexpected impediment to attaining favorable opinions on statements.”

developed a viable and efficient division of labor. The OIG, DoD, provides oversight of Military Department financial audits, and there are no valid grounds for questioning the objectivity and independence of the Military Department auditors, as demonstrated by the dozens of critical reports and

disclaimers of opinion issued by them over the past decade. Forcing a diminished role for the Service auditors, merely to satisfy a questionably necessary standard, could pose another significant and unexpected impediment to attaining favorable opinions on statements.

OIG, DoD, Testimony

The Deputy Inspector General testified on Defense Management Challenges before the House Budget Committee on February 17, 2000. He identified the main challenge areas confronting the Department as:

- Information Technology Management
- Information Security
- Other Security Concerns
- Financial Management
- Acquisition
- Health Care
- Supply Inventory Management
- Other Infrastructure Issues
- Readiness
- Turbulence from Change

On March 16, 2000, the Assistant Inspector General for Auditing testified before the House Subcommittee on Government Management, Information and Technology regarding Defense acquisition programs. The testimony stressed IG concern about the acquisition workforce and training, contracting for services and spare parts pricing issues.

On March 23, 2000, the Deputy Inspector General discussed the National Security Implications of Export Controls and the Export Administration

Act of 1999, S. 1712, in testimony to the Senate Armed Services Committee. He reiterated the strong support of the OIG, DoD, for renewal of the Export Administration Act, but suggested a number of improvements to S. 1712. The primary suggestions related to procedures for license exceptions, the standard for when controls may be imposed, the role of the Secretary of Defense in decision making on matters such as commodity classification requests, the interagency appeals process and time limits for processing license applications.

The full text of the written testimony for these hearings is available at www.dodig.osd.mil.

INTELLIGENCE REVIEW

Figure 6 is a statistical summary of reports issued dealing with intelligence oversight. For information regarding specific work performed, see the Classified Annex to this report.

Intelligence Oversight				
Organizations	OIG, DoD	Military Depts	Defense Agencies	Totals
Intelligence Programs and Operations				
Operations and Support	5	4	12	21
Financial Management	2	1	4	7
Acquisition and Contract Management	3	1	2	6
Computer Management/Information Technology	5	0	4	9
Management Oversight	1	0	7	8
Management/Criminal Investigations	0	2	5	7
Special Emphasis Area				
Information Assurance	0	0	1	1
Total	16	8	35	59

Figure 6

This page left blank intentionally

APPENDIX A*

REPORTS ISSUED BY CENTRAL DOD INTERNAL AUDIT ORGANIZATIONS

Excludes base level reports issued by the Air Force Audit Agency. Includes evaluation reports issued by the OIG, DoD.

Copies of reports may be obtained from the appropriate issuing office by calling:

OIG, DoD
(703) 604-8937

Army Audit Agency
(703) 681-9863

Naval Audit Service
(202) 433-5737

Air Force Audit Agency
(703) 696-8027

Summary of Number of Reports by Issue Area October 1, 1999 through March 31, 2000

	OIG, DoD	Military Depts.	Total
Acquisition Oversight	16	9	25
Construction and Installation Support	2	4	6
Environment	3	7	10
Finance and Accounting	23	34	57
Health Care	2	2	4
Information Technology	29	6	35
Intelligence	0	1	1
Logistics	4	17	21
Quality of Life	2	15	17
International Security	1	4	5
Total	82	99	181
The OIG, DoD, also issued 3 reports on audit oversight reviews (D2000-6-001, D2000-6-002, and D2000-6-003).			

*Fulfills requirements of 5 U.S.C., Appendix 3, Section 5(a)(6).

ACQUISITION PROGRAM AND CONTRACTOR OVERSIGHT

IG, DoD

00-003 The Air Force Contract Audit Followup System (10/4/99)

00-019 Procurement Practices for the Composite Armored Vehicle and Composite Affordability Initiative Programs (10/26/99)

D-2000-055 Acquisition Management of the Joint Total Asset Visibility System (12/14/99)

D-2000-059 Allegations Relating to the Security Controls on Two Air Force Programs (12/16/99)

D-2000-061 Ballistic Missile Defense Organization Technology Selection Process for the Discriminating Interceptor Technology Program Laser Radar (12/17/99)

D-2000-065 Costs Charged to Other Transactions (12/27/99)

D-2000-075 Administration and Management of the Civil Air Patrol (2/15/00)

D-2000-088 DoD Acquisition Workforce Reduction Trends and Impacts (2/29/00)

D-2000-092 Acquisition of the Minuteman III Propulsion Replacement Program (3/1/00)

D-2000-098 Spare Parts and Logistics Support Procured on a Virtual Prime Vendor Contract (3/8/00)

D-2000-099 Procurement of the Propeller Blade Heaters for the C-130 and P-3 Aircraft (3/8/00)

D-2000-100 Contracts for Professional, Administrative, and Management Support Services (3/10/00)

D-2000-102 Military Working Dog Procurements (3/14/00)

D-2000-107 Navy Acquisition of Air Membrane Dehydrators (3/23/00)

D-2000-108 Radioactive Material Containment Bags (3/22/00)

D-2000-079 Summary of the DoD Process for Developing Quantitative Munitions Requirements (2/24/00)

Army Audit Agency

AA 00-16 Tank Training Devices for National Guard Units (11/1/99)

AA 00-29 Use of International Merchant Purchase Authorization Cards (IMPAC) (11/10/99)

AA 00-28 Use of International Merchant Purchase Authorization Cards (IMPAC) (11/12/99)

Naval Audit Service

N2000-0015 Program Executive Office Auditor Project (1/25/00)

Air Force Audit Agency

98064003 Airborne Laser Program Integrated Product Team Participation (12/8/99)

98064017 Air-to-Air Weapon System Evaluation Program (12/6/99)

98064024 Award Fee Management on Commercial Activity Contracts (3/27/00)

99064008 Acquisition of Commercial Spare Parts (1/24/00)

99064019 Service Contracting Quality Assurance Evaluation Program (1/12/00)

CONSTRUCTION AND INSTALLATION SUPPORT

IG, DoD

D-2000-064 Defense Base Realignment and Closure Budget Data for Various Projects Realigned From Kelly Air Force Base to Lackland Air Force Base, Texas (12/21/99)

D-2000-074 Budget Data for Realignment of Gas Systems Test Cells From Kelly Air Force Base to Hill Air Force Base (2/10/00)

Army Audit Agency

AA 00-96 Flood Damage Assessment (1/20/00)

AA 00-163 Program Assessment and Execution-FY 99 Flood Damage Funds (2/24/00)

Naval Audit Service

N2000-0002 Military Construction, Navy Projects Proposed for Fiscal Year 2001 (10/19/99)

Air Force Audit Agency

99052009 Infrastructure Reduction (11/19/99)

ENVIRONMENT

IG, DoD

00-012 Hazardous Material Management for the F-15 Aircraft Program (10/15/99)

00-020 Hazardous Waste Disposal Costs for the Defense Logistics Agency (10/26/99)

00-022 Hazardous Material Management for the Nimitz-Class Nuclear Aircraft Carrier Program (10/27/99)

Army Audit Agency

AA 00-110 Hazardous Waste Disposal Volumes and Costs (12/27/99)

AA 00-122 Execution of Environmental Projects (12/30/99)

AA 00-174 Execution of the Installation Restoration Program (2/28/00)

Naval Audit Service

N2000-0012 Replacement/ Conversion of Equipment Using Class 1 Ozone Depleting Substances at Selected Navy Shore Installations (12/10/99)

N2000-0013 Environmental Cleanup at Hunters Point Shipyard, San Francisco, CA (12/21/99)

Air Force Audit Agency

99052015 Air Installation Compatible Use Zone Program Management (11/1/99)

99052016 Affirmative Procurement Program (11/23/99)

FINANCE AND ACCOUNTING

IG, DoD

00-011 Compilation of Defense Logistics Agency Cash Transactions (10/18/99)

00-023 Compilation Of Defense Reutilization and Marketing Service Operating Results (10/28/99)

00-027 Automated Systems Used to Prepare the Defense Logistics Agency Working Capital Fund Financial Statements (10/28/99)

D-2000-030 Recording Obligations in Official Accounting Records (11/4/99)

D-2000-041 Deficiencies in FY 1998 DoD Financial Statements and Progress Toward Improved Financial Reporting (11/26/99)

D-2000-044 Reconciliation of Differences Reported for Checks Issued by the Defense Finance and Accounting Service Columbus Center Disbursing Stations (11/30/99)

D-2000-069 FY 1998 Department of Defense Agency-Wide Statement of Budgetary Resources (12/29/99)

D-2000-071 Maintenance and Repair of DoD General and Flag Officer Quarters (1/27/00)

D-2000-080 Inspector General, DoD, Oversight of the Army Audit Agency Audit of the FY 1999 Army Working Capital Fund Financial Statement Audit (2/17/00)

D-2000-081 Inspector General, DoD, Oversight of the Naval Audit Service Audit of the FY 1999 Department of the Navy General Fund Financial Statements (2/14/00)

D-2000-082 Inspector General, DoD, Oversight of the Naval Audit Service Audit of the FY 1999 Department of the Navy Working Capital Fund Financial Statements (2/14/00)

D-2000-083 Inspector General, DoD, Oversight of the Air Force Audit Agency Audit of the FY 1999 Air Force Working Capital Fund Financial Statements (2/14/00)

D-2000-084 Inspector General, DoD, Oversight of the Air Force Audit Agency Audit of the FY 1999 Air Force General Fund Financial Statements (2/14/00)

D-2000-085 Inspector General, DoD, Oversight of the Audit of the Military Retirement Fund Financial Statements for FY 1999 (2/15/00)

D-2000-087 Inspector General, DoD, Oversight of the Army Audit Agency Audit of the Army's General Fund Principal Financial Statements for Fiscal Year 1999 (2/14/00)

D-2000-090 Inpatient Data Supporting the DoD Military Retirement Health Benefits Liability Estimate (3/1/00)

D-2000-091 Internal Controls and Compliance With Laws and Regulations for the DoD Agency-Wide Financial Statements for FY 1999 (2/25/00)

D-2000-093 Inspector General, DoD, Oversight of the Army Audit Agency Audit of the FY 1999 U.S. Army Corps of Engineers, Civil Works Program, Financial Statements (2/28/00)

D-2000-095 Internal Controls and Compliance With Laws and Regulations for the Defense Logistics Agency Working Capital Fund Financial Statements for FY 1999 (2/29/00)

D-2000-097 Accounting Procedures and Controls Over Financial Data Supporting Other Defense Organizations (3/9/00)

D-2000-103 Internal Controls and Compliance With Laws and Regulations for the FY 1999 Financial Statements for Other Defense Organizations-General Funds (3/16/00)

D-2000-104 Controls Over Obligations at Washington Headquarters Services (3/22/00)

D-2000-078 Reliability of the Defense Commissary Agency Personal Property Database (2/18/00)

Army Audit Agency

AA 00-19 Army Working Capital Fund FY 98 Financial Statements-Fund Balance With Treasury (10/15/99)

AA 00-48 Army Working Capital Fund FY 98 Financial Statements-Statement of Budgetary Resources (10/29/99)

AA 00-3 Headquarters, DA Redesign Efficiency (11/4/99)

AA 00-25 Funding for Unmanned Aerial Vehicles (11/5/99)

AA 00-27 Integrated Logistics Analysis Program Efficiency (11/8/99)

AA 00-21 Expenditures for Aviation Fuel (11/16/99)

AA 00-63 Army Working Capital Fund FY 98 Financial Statements-Inventory Allowance Accounts (11/17/99)

AA 00-168 Army's General Fund Principal Financial Statements for Fiscal Year 1999-Summary Audit Report (2/9/00)

AA 00-177 Army Working Capital Fund Principal Financial Statements for Fiscal Year 1999-Auditor's Report (2/10/00)

AA00-178 Army Working Capital Fund Principal Financial Statements for Fiscal Year 1999-Internal Controls and Compliance With Laws and Regulations (2/17/00)

AA 00-186 FY 99 Financial Statements (2/18/00)

AA 00-190 Unexpended Appropriations-Army Working Capital Fund FY 99 Financial Statements (2/28/00)

AA 00-202 Internal Controls Over Selected Revenue, Expense, and Equity Accounts (3/22/00)

AA 00-205 Military Interdepartmental Purchase Requests (3/27/00)

AA 00-218 Internal Controls Over Obligations, Disbursements, Orders Received, and Collected (3/29/00)

Naval Audit Service

N2000-0005 Department of the Navy Principal Statements for Fiscal Year 1998: Selected Payments and Collections (10/29/99)

N2000-0008 Auditor General Opinion: Department of the Navy Annual Statement of Assurance for Fiscal Year 1999 (11/10/99)

N2000-0014 Department of the Navy Working Capital Fund Inventory Records and Valuation (12/30/99)

N2000-0016 Validation of Selected Work Request Obligations in the Standard Accounting and Reporting System (1/28/00)

N2000-0018 Department of the Navy Principal Statements for Fiscal Year 1999 (2/10/00)

N2000-0019 Fiscal Year 1999 Consolidated Financial Statements of the Department of the Navy Working Capital Fund (2/14/00)

Air Force Audit Agency

98053001 Accounting for Selected Assets and Liabilities-Fund Balance With Treasury, Fiscal Year 1998 (1/6/00)

99052030 United States Air Force Academy General Officer Quarters (10/26/99)

98053005 Accounting for Fiscal Year 1998 Air Force Liabilities (11/19/99)

98053006 Accounting for Air Force Real Property, Fiscal Year 1998 (12/22/99)

98054032 Internal Controls Over Purchases of Goods and Services (2/23/00)

99053002 Opinion on Fiscal Year 1999 Air Force Consolidated Financial Statements (2/9/00)

99054002 Selected Civilian Pay Entitlements (3/1/00)

99054006 Official Representation Funds (10/15/99)

99054008 First and Second Destination Transportation Centrally Managed Allotments (2/10/00)

99054014 Support Agreement Reimbursements (10/29/99)

99054026 Audit Results, Selected Aspects of the Air Force Reserve Travel System (2/14/00)

99054028 Memorandum Report, Controls in the Status of Funds System (10/20/99)

99068011 Opinion on Fiscal Year 1999 Air Force Working Capital Fund Financial Statements (2/9/00)

HEALTH CARE

IG, DoD

00-010 Administration and Management of the Armed Forces Institute of Pathology (10/15/99)

00-016 TRICARE Marketing (10/21/99)

Army Audit Agency

AA 00-160 Military Treatment Facility Downsizing and Health-care for Soldiers in Remote Locations (2/18/00)

AA 00-179 Health Care for DA Civilians Stationed Overseas (3/3/00)

INFORMATION TECHNOLOGY RESOURCES

IG, DoD

00-001 Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility: Alaskan Command (10/1/99)

00-002 Year 2000 End-to-End Testing: Logistics Capstone Plan (10/1/99)

00-004 U.S. European Command Year 2000 Operational Readiness (10/8/99)

00-006 Defense Disbursing Year 2000 End-to-End Testing (10/12/99)

00-007 Defense Transportation Pay Year 2000 End-to-End Testing (10/12/99)

00-015 Year 2000 Higher Level Testing Schedule Data Reported to DoD (10/20/99)

00-017 Defense Military Pay Year 2000 End-to-End Testing (10/21/99)

00-018 Defense Travel Pay Year 2000 End-to-End Testing (10/22/99)

00-021 Air Force Logistics Year 2000 End-to-End Test Planning (10/26/99)

00-025 End-to-End Testing for Personnel Systems (10/26/99)

00-026 Joint Operation Planning Year 2000 Issues (10/27/99)

D-2000-029 Year 2000 Contingency Planning and Operational Evaluation Reporting by U.S. Forces Korea (11/1/99)

D-2000-031 Year 2000 End-to-End Tests for the Military Health System (11/4/99)

D-2000-032 Year 2000 Status of the Compliance Monitoring and Tracking System (11/5/99)

D-2000-033 Army Logistics Year 2000 End-to-End Test Planning (11/5/99)

D-2000-035 Procurement Systems Year 2000 End-to-End Test (11/9/99)

D-2000-036 Defense Logistics Agency Logistics Year 2000 End-to-End Test Planning (11/12/99)

D-2000-040 Navy Logistics Year 2000 End-to-End Test Planning (11/16/99)

D-2000-042 Year 2000 Operational Contingency Planning for Health Care in the European Theater (11/26/99)

D-2000-043 Air Force Level I Logistics Year 2000 End-to-End Test Planning (11/29/99)

D-2000-046 Year 2000 Computing Issues Related to Health Care in DoD-Phase III (12/1/99)

D-2000-048 Year 2000 Compliance Status of Biomedical Devices Included in Navy Fleet Hospitals (12/3/99)

D-2000-049 DoD Year 2000 Contingency Plans (12/10/99)

D-2000-057 Summary of DoD Year 2000 Issues IV (12/16/99)

D-2000-058 Identification and Authentication Policy (12/20/99)

D-2000-060 Year 2000 Contingency Plans for Personnel Systems (12/16/99)

D-2000-063 Information Technology Funding in the Department of Defense (12/17/99)

D-2000-066 Communication Systems Year 2000 End-to-End Tests (12/23/99)

D-2000-068 Year 2000 Conversion Program for Defense Critical Suppliers (12/28/99)

Army Audit Agency

AA 00-1 Information Assurance-Phase III: Funding and Performance Measures (12/14/99)

AA 00-116 Installation Telecommunications Switches (1/20/00)

AA 00-214 Summary of Year 2000 Audit Coverage-Lessons Learned (3/31/00)

Navy Audit Service

N2000-0017 Management of Long-Haul Telecommunications Circuits in the San Diego, CA Region (1/31/00)

Air Force Audit Agency

99066013 Certification and Accreditation of Pacific Air Forces Information Systems (3/1/00)

99066019 Information Protection - Implementing Controls Over Known Vulnerabilities in Air Force Materiel Command Computers (FOR OFFICIAL USE ONLY) (3/2/00)

INTELLIGENCE

See Appendix in Classified Annex to this report.

LOGISTICS

IG, DoD

D-2000-050 Disposal of Munitions Items at Fort Irwin (12/8/99)

D-2000-054 Cash Impact of the Consumable Item Transfer, FY 1999 (12/14/99)

D-2000-056 DoD Electronic Mail Implementation Planning (12/15/99)

D-2000-086 Assuring Condition and Inventory Accountability of Chemical Protective Suits (2/25/00)

Army Audit Agency

AA 00-4 Repair of Secondary Items (10/29/99)

AA 00-76 Process for Determining Source of Depot Level Maintenance (12/14/99)

AA 00-77 Process for Determining Source of Depot Level Maintenance (12/14/99)

AA 00-107 Process for Determining Source of Depot Level Maintenance (1/3/00)

AA 00-111 Process for Determining Source of Depot Level Maintenance (1/20/00)

AA 00-131 Demilitarization of Conventional Ammunition (2/4/00)

AA 00-153 Material Weakness Plan for the Manpower Requirements Determination System (2/15/00)

AA 00-185 Integrated Sustainment Maintenance Program (3/8/00)

AA 00-199 Contracting for Field-Level Maintenance of Tactical Equipment (3/14/00)

AA 00-147 Manpower Requirements Criteria-Maintenance and Support Personnel (3/22/00)

Navy Audit Service

N2000-0001 Management of Advanced Equipment Repair Program and Trident Planned Equipment Replacement Program (10/12/99)

N2000-0003 Energy Conservation at the Naval Air Station, Patuxent River, MD (10/19/99)

N2000-0006 Marine Corps Retail Supply Management of Material Returns (12/29/99)

N2000-0007 Recording Onhand Quantities of Aviation Depot Level Repairable Inventories at Commercial Contractor Repair Facilities (10/29/99)

Air Force Audit Agency

99061005 F110-GE-100 Spare Engine and Upgrade Requirements (1/12/00)

99061026 Followup Audit,
Noncataloged Depot Item
Management (11/2/99)

99062015 Aircraft External
Fuel Tank Build-Up Program
(12/15/99)

QUALITY OF LIFE

IG, DoD

D-2000-076 Allegations on the
Air Force Promotion Process for
Officers Working on Special
Access Programs (2/16/00)

D-2000-101 Report on the
Military Environment With
Respect to the Homosexual
Conduct Policy (3/16/00)

Army Audit Agency

AA 00-18 Barnes Post
Restaurant Fund (10/29/99)

AA 00-30 Billeting Financial
Operations (11/4/99)

AA 00-31 Financial Controls
Over Morale, Welfare and
Recreation Activities (11/4/99)

AA 00-68 Reengineering
Overhead Support for Morale,
Welfare and Recreation
Activities (11/30/99)

AA 00-130 Army Executive
Dining Facility Fund Financial
Statements (1/4/00)

AA 00-53 Secretary of Defense
Mess Fund Financial Statements
(1/6/00)

Naval Audit Service

N2000-0009 Combined
Bachelor Quarters Operations at
the Naval Air Station, Patuxent
River, MD (11/16/99)

N2000-0004 Funding and
Requirements Determination for
Temporary Duty Under Instruc-
tion as Related to Permanent
Change of Station Moves
(10/19/99)

N2000-0010 Naval Reserve
Headquarters Staffs (11/18/99)

N2000-0011 Marine Corps
Recruiting Functions (12/1/99)

Air Force Audit Agency

99058013 Bare Base Set
Requirements (U)
(CLASSIFIED) (1/4/00)

98051020 Base Capital
Improvement Fund Use
(12/20/99)

99051007 Safety of Life in
Confined Spaces (2/28/00)

99051026 Ground Safety
Program Costs (3/14/00)

99051033 Air National Guard
Safety of Life in Confined
Spaces (3/2/00)

INTERNATIONAL SECURITY

IG, DoD

D-2000-110 Export Licensing
at DoD Research Facilities
(3/24/00)

Army Audit Agency

AA 00-33 Technology Trans-
fers for Classified and Sensitive
Information (12/20/99)

AA 00-141 Technology
Transfers in Special Programs
(1/18/00)

AA 00-32 Army Foreign
Language Program Require-
ments (2/14/00)

Air Force Audit Agency

99062008 Reduced-Price
Foreign Military Sales and
Related Grant Transactions
(3/28/00)

AUDIT OVERSIGHT REVIEWS

IG, DoD

D-2000-6-001 Pricewaterhouse
Coopers L.L.P., and the Defense
Contract Audit Agency
California Institute of Tech-
nology, Fiscal Year Ended
September 30, 1996 (11/19/99)

D-2000-6-002 Pricewaterhouse
Coopers L.L.P., and the Defense
Contract Audit Agency
California Institute of
Technology, Fiscal Year Ended
September 30, 1999 (11/19/99)

D-2000-6-003 Office of the
Inspector General, Defense
Intelligence Agency (2/14/00)

Our report on the status of OIG, DoD, reports over 12 months old in which management decisions have been made but final action has not been taken has been provided to the Department and is available upon request.

APPENDIX B*
INSPECTOR GENERAL, DoD, AUDIT REPORTS ISSUED CONTAINING
QUANTIFIABLE POTENTIAL MONETARY BENEFITS

Audit Reports Issued	Potential Monetary Benefits	
	Disallowed Costs¹	Funds Put to Better Use
D-2000-023 Compilation of Defense Reutilization and Marketing Service Operating Results (10/28/99)	N/A	\$529,600,000
D-2000-098 Spare Parts and Logistics Support Procured on a Virtual Prime Vendor Contract (3/8/00)	N/A	29,400,000
D-2000-099 Procurement of the Propeller Blade Headers for the C-130 and P-3 Aircraft (3/8/00)	N/A	5,600,000
Totals	0	\$564,600,000
¹ There were no OIG audit reports during the period involving disallowed costs.		

*Fulfills the requirement of 5 U.S.C., Appendix 3, Section 5(a)(6).

This page left blank intentionally

APPENDIX C*
FOLLOWUP ACTIVITIES

DECISION STATUS OF INSPECTOR GENERAL ISSUED REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE¹ (\$ in thousands)		
Status	Number	Funds Put to Better Use
A. For which no management decision had been made by the beginning of the reporting period.	30	\$33,300
B. Which were issued during the reporting period.	110	564,600
Subtotals (A+B)	140	597,900
C. For which a management decision was made during the reporting period.	109	25,400
(i) dollar value of recommendations that were agreed to by management		
- based on proposed management action		4,200
- based on proposed legislative action		4,200
(ii) dollar value of recommendations that were not agreed to by management		21,200
D. For which no management decision has been made by the end of the reporting period.	31	572,500
Reports for which no management decision was made within 6 months of issue (as of March 31, 2000). ²	6	7,900
¹ There were no OIG audit reports during the period involving questioned costs. ² OIG Report No. 99-064, "Basis for Recent Policy Changes to the Drug Testing Rate for DoD Civilians," issued December 31, 1998; OIG Report No. 99-102, "Chemical and Biological Warfare Defense Resources in the U.S. European Command," issued March 4, 1999; OIG Report No. 99-106, "Commercial Life Insurance Sales Procedures in DoD," issued March 10, 1999; and OIG Report No. 99-135, "Trends and Progress in Reducing Problem Disbursements and In-Transit Disbursements," issued April 16, 1999, had no management decisions made within 6 months of issuance and mediation is ongoing. OIG Report No. 99-166, "Initial Implementation of the Standard Procurement System," was issued May 26, 1999, and decided April 7, 2000. Navy Audit Service Report No. 052-98, "Department of the Navy Principal Statements for Fiscal Years 1997 and 1996: Fund Balance," was issued September 30, 1998, and was decided April 26, 2000.		

*Fulfills requirements of 5 U.S.C., Appendix 3, Section 5(a)(8)(9) and Section 5(b)(2)(3).

STATUS OF ACTION ON CENTRAL INTERNAL AUDITS ¹ (\$ in thousands)		
Status of Action	Number of Reports	Funds Put to Better Use
OIG, DoD		
Action in Progress - Beginning of Period	308	\$13,379
Action Initiated - During Period	109	4,200
Action Completed - During Period	131	6,009
Action in Progress - End of Period ²	286	7,810
Military Departments		
Action in Progress - Beginning of Period	360	4,740,789
Action Initiated - During Period	133	271,644
Action Completed - During Period	86	279,429
Action in Progress - End of Period	407	4,475,732
¹ There were no audit reports during the period involving questioned costs.		
² On certain reports (primarily from prior periods) with audit estimated monetary benefits of \$379 million, it has been agreed that the resulting monetary benefits can only be estimated after completion of management action, which is ongoing.		

APPENDIX D
CONTRACT AUDIT REPORTS ISSUED*
(\$ in millions)

Type of Audit	Reports Issued	Examined	Audit Exceptions	Funds Put to Better Use
Incurring Costs ¹	9,700	\$37,943.3	\$439.7	\$119.8
Forward Pricing Proposals	4,188	34,179.3	--	1,992.2
Cost Accounting Standards	1,017	319.3	73.5	--
Defective Pricing ²	218	--	2.9	--
Other ³	1	--	--	--
Totals	15,124	\$72,441.9	\$516.1	\$2,112.0
¹ Incurring cost funds put to better use are from the cost avoidance recommended in economy and efficiency audits of contractor operations.				
² Defective pricing dollars examined are not reported because they are considered a duplication of forward pricing dollars reported as examined.				
³ Relates to suspected irregular conduct cases.				

*Because of limited time between availability of management information system data and legislative reporting requirements, there is minimal opportunity for the DCAA to verify the accuracy of reported data. Accordingly, submitted data is subject to change based on subsequent DCAA authentication.

Waivers of Advisory and Assistance Service Contracts

A review is made of each waiver of advisory and assistance services contracts granted by the Department. This review is required by Section 802, Defense Authorization Act for Fiscal Year 1990.

The Department made no waivers during the period and therefore, no reviews were made by the OIG.

This page left blank intentionally